

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioFILED  
RICHARD W. NAGEL  
CLERK OF COURT

2017 SEP 29 AM 11:14

U.S. DISTRICT COURT  
SOUTHERN DIST. OHIO  
SHARON L. OVINGTONIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)2002 Dark colored Lexus S43 convertible bearing  
Oregon license plate CU 21010

Case No.

**3 : 17 mj 456****SHARON L. OVINGTON**

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A-2

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):


- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC s. 1030(a)(2)	- attempt to intentionally access a computer without authorization
18 USC s. 1030(a)(4)	- knowingly & with the intent to defraud attempt to access a protected computer
18 USC s. 1030(a)(7)	- intent to extort a thing of value

The application is based on these facts:  
See Attached Affidavit of Nicholas Graziosi

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Nicholas Graziosi, Special Agent of the FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

9-29-17

City and state: Dayton, Ohio



Judge's signature

Sharon L. Ovington, US Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS**

I, Nicholas Graziosi, a Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. I have been employed as a Special Agent of the Federal Bureau of Investigation since March 2017, and am currently assigned to the Cincinnati Division. Prior to my employment at the Federal Bureau of Investigation, I was enlisted with the United States Marine Corp and later earned a law degree from West Virginia University College of Law. While employed by the Federal Bureau of Investigation, I have investigated various violation of federal criminal law. I have also spoken with and received information from experienced FBI special agents who investigate cybercrimes, including the use and installation of malware on protected computer systems.
2. I make this affidavit in support of an application for a search warrant for the following as evidence, contraband, fruits of a crime, other items illegally possessed as well as property designed for use, intended for use, or used in committing violations of, among other things, 18 U.S.C. § 1030 (a)(2) (attempt to intentionally access a computer without authorization or exceeds authorized access); 18 U.S.C. § 1030 (a)(4) (attempt to knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access); and 18 U.S.C. § 1030 (a)(7) (intent to extort a thing of value) exists and can be found at the following location:
  - a. The residential property located at the Xenia Country Inn, 38 S. Allison Avenue, Room 254, Xenia, Ohio 45385 (hereinafter referred to as "SUBJECT PREMISES", and more fully described in Attachment A-1);
  - b. A 2002 Dark colored Lexus S43 convertible bearing Oregon license plate CU 21010, (hereinafter referred to as "SUBJECT VEHICLE", and more fully described in Attachment A-2);
  - c. All electronic devices and documents found in the possession of CHRISTOPHER PAUL MURPHY, aka SAMUEL GOODWIN;
3. I also make this affidavit in support of an application for an anticipatory search for the following as evidence, contraband, fruits of a crime, other items illegally possessed as well as property designed for use, intended for use, or used in committing violations of, among other things, 18 U.S.C. § 1030 (a)(2) (attempt to intentionally access a computer without authorization or exceeds authorized access); 18 U.S.C. § 1030 (a)(4) (attempt to knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access); and 18 U.S.C. § 1030 (a)(7) (intent to extort a thing of value) exists and can be found at the following location:
  - a. Any electronic storage devices or electronic devices that CHRISTOPHER PAUL MURPHY, aka SAMUEL GOODWIN may provide to the individual identified



herein as the CHS for the purpose of installing malware or other computer programs at Nationwide BiWeekly Administration, Inc.(NBA) if and only if CHRISTOPHER PAUL MURPHY, aka SAMUEL GOODWIN any electronic storage devices or electronic devices to the CHS at their planned meeting on or about October 2, 2017.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.
5. This investigation pertains to attempted computer intrusion and theft of proprietary client and/or customer information from a Xenia-based company that would result in at least over \$900,000 in potential losses to the company.

#### **PERTINENT FEDERAL CRIMINAL STATUTES**

6. 18 U.S.C. § 1030 (a)(2) states that it is a violation for any person to intentionally access a computer without authorization or exceeds authorized access, and thereby obtains:
  - a. Information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a field of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
  - b. Information from any department or agency of the United States; or
  - c. Information from any protected computer.
7. 18 U.S.C. § 1030 (a)(4) states that it is a violation for any person to knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is no more than \$5,000 in any 1-year period.
8. 18 U.S.C. § 1030 (a)(7) states that it is a violation for any person with the intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any –
  - a. Threat to cause damage to a protected computer;
  - b. Threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained

from a protected computer without authorization or by exceeding authorized access; or

- c. Demand or request money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.
9. 18 U.S.C. § 1030 (b) states that it is a violation for any person who conspires to commit or attempts to commit an offense under 1030(a).
10. For purposes of these statutes, the term “protected computer” is defined in 18 U.S.C. § 1030(e)(2) as:
- a. A computer exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or Government; or
  - b. A computer which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

11. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.
12. There is probable cause to believe that things that were once stored on the device may still be stored there, for at least the following reasons:
- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
  - b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In



addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
  - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
13. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
  - b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
  - c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
  - d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
  - f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.
14. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

#### **PROBABLE CAUSE**

15. Nationwide BiWeekly Administration, Inc.(NBA), located in Xenia, OH, is an Ohio-based company that transmits funds from consumers to their mortgage servicers to facilitate biweekly payment of mortgages.
16. In September 2017, a confidential human source (CHS) previously employed by NBA was approached by an individual identifying himself as SAMUEL GOODWIN from AAA Financial Corp. (AAA), 900 Semple Road #301, Coral Springs, Florida, 954-859-4227, <http://aaafinancial.com>. The individual identifying himself as GOODWIN offered the CHS \$14,000 to gain entry to the NBA office, receive an email on the CHS's work email account, open the attached file on the email, and copy the resultant client data from NBA to a thumb drive and deliver the drive to GOODWIN. In short, GOODWIN intended to have the CHS assist him install some type of malware or other malicious program on NBA's computer system to collect client data.
17. GOODWIN also explained to the CHS that if the email attachment did not work, he could also provide the CHS with a thumb drive containing the malware. GOODWIN



explained that the data taken from NBA would be used for GOODWIN to contact the clients and attempt to start providing services to NBA's clients.

18. Based on a photographic lineup, the CHS picked GOODWIN's photograph out. The individual the CHS identified as GOODWIN was in reality CHRISTOPHER PAUL MURPHY, date of birth in 1949 with a home address 2533 S. Apache Road, Golden Valley, Arizona.
19. Open source research has shown that 2533 Apache Road, Golden Valley, Arizona is the address for a company called Bi-Weekly Mortgage Association.
20. At a follow-up consensually recorded meeting on September 20, 2017 with the CHS, MURPHY agreed to pay the CHS \$1000 up front upon delivering the thumb drive with malware, with the remaining \$13,000 to be paid later. MURPHY also agreed to double the pay that the CHS received in the past from NBA. During the meeting, MURPHY also told the CHS that the email to be sent to the CHS could be made to come from anybody, including management personnel at NBA. MURPHY stated that he could have the sending email address cloned or cloaked to make it appear to come from a different person. MURPHY further explained that all the CHS would need to do is take the \$1000 payment, go into NBA, get the email, open it, minimize it, and walk away. MURPHY's statements indicate that he intended to use the CHS to improperly gain access to NBA's computer system and obtain its protected client data and/or information.
21. Prior to the September 20th meeting, your affiant and other FBI agents witnessed MURPHY arrive for the meeting driving a dark colored Lexus convertible with Oregon plates CU21010, i.e., the SUBJECT VEHICLE. Records checks showed this to be registered to MURPHY.
22. Immediately following the September 20<sup>th</sup> meeting, FBI agents witnessed MURPHY leave the meeting place and drive directly to the Xenia Country Inn, 38 S. Allison Avenue, Xenia, Ohio 45385. MURPHY parked his vehicle immediately in front of unit #254, i.e., the SUBJECT PREMISES, and entered the door immediately in front of the vehicle, labeled as room 254. It should be noted that MURPHY represented to the CHS that he (MURPHY) had been in the Xenia area for approximately 2 months. I also conducted a spot check at the SUBJECT PREMISES on September 28, 2017 and observed the SUBJECT VEHICLE parked directly in front of Room 254.
23. Since the September 20, 2017 meeting, MURPHY and the CHS have had periodic contact with one another. During their communications, at the direction of FBI, the CHS agreed to meet with MURPHY and obtain from him the electronic device containing the suspected malware. MURPHY and the CHS currently plan to meet with one another in the Dayton, Ohio area on October 2, 2017 to complete this transaction. Given MURPHY's previous statements to the CHS, I anticipate that he will deliver to the CHS at the October 2, 2017 meeting some type of electronic device containing malware or

some other type of computer program designed to improperly collect or take data from NBA.

24. Based on my training and experience as well as discussions with experience cyber agents, I know that people engaged in conduct such as MURPHY often carry with them electronic devices, electronic media, cellular telephones, as well as multiple copies of the malware or executable file. Additionally, individuals engaged in this type of cyber theft often do not work alone and obtain the malware or computer from experience cyber criminals. In doing so, they often will have in their possession contact information or communications with these cyber criminals. Moreover, given that MURPHY reached out to at least one former employee of NBA – namely, the CHS, it is likely that he has in possession contact information of other current and former employees of the company. MURPHY may have contacted other NBA personal via email or the use of a cellular telephone, which he has used to text the CHS. Given his familiarity with NBA, he likely has in his possession information and other documents relating to that company, its products and services. MURPHY has represented that he has been in this area for an extended period of time. He likely possessed with him information concerning the duration and locations of his travels. Based on my training and experience, I know that, when traveling such as MURPHY has been, individuals often keep the aforementioned items in their motel rooms and vehicles. I also know that individuals frequently carry electronic devices on their person.



**CONCLUSION**

25. Based on the aforementioned information, I request that the Court issue the proposed search warrant. Because the warrant for devices in the possession of MURPHY will be served at a time and location determined at the availability and willingness of CHS and MURPHY, and the circumstances surrounding the meeting, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

**REQUEST FOR SEALING**

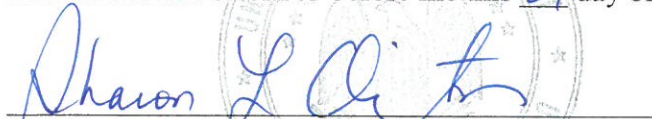
26. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Nicholas Graziosi  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this 29<sup>th</sup> day of September 2017:

  
THE HONORABLE SHARON L. OVINGTON  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A-1**

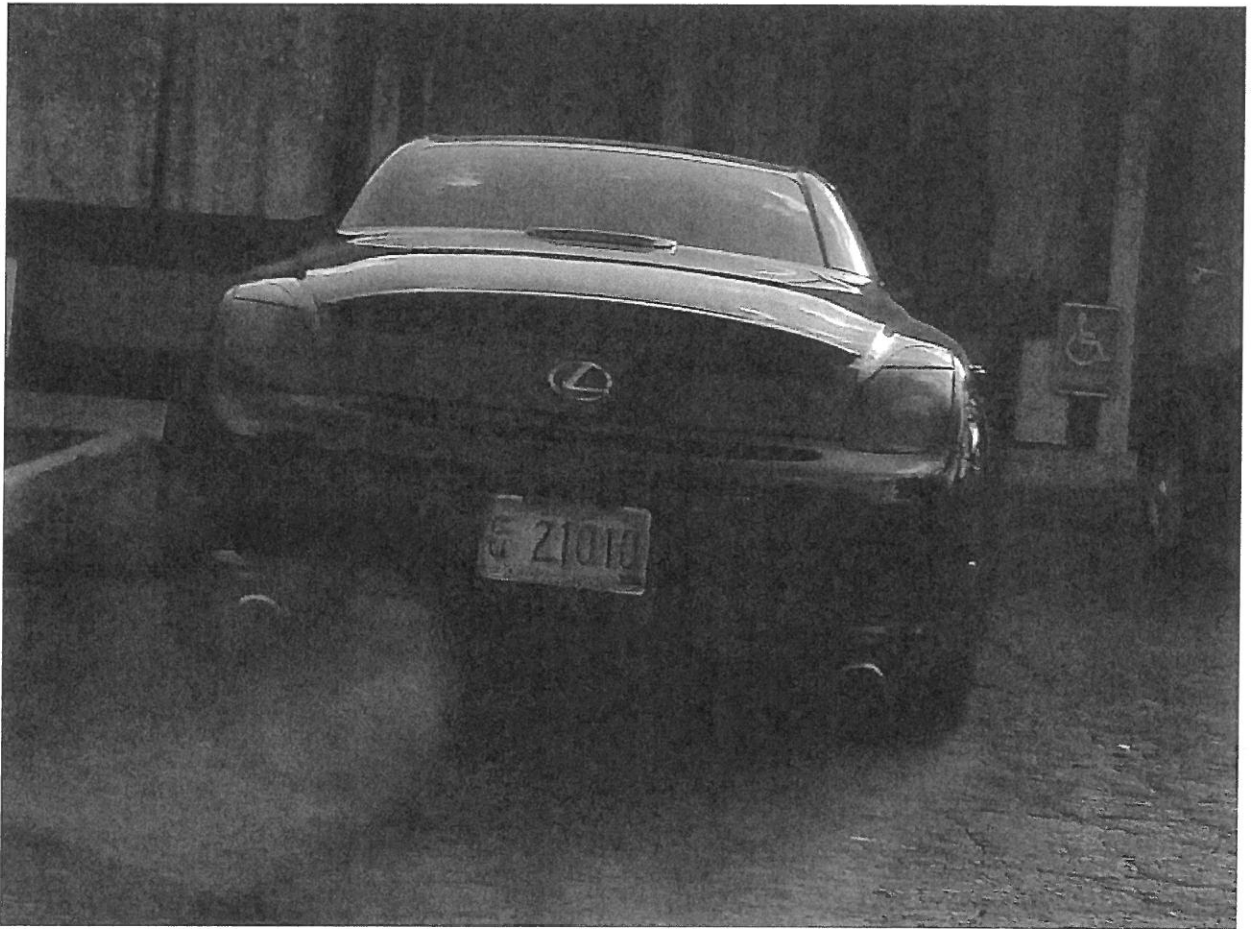
38 S. Allison Avenue, #254, Xenia, Ohio 45385 is a motel room at the Xenia Country Inn. The room is labeled with numbers "254" immediately to the left of the door.





ATTACHMENT A-2

The vehicle is described as a 2002 dark colored Lexus S43, bearing Oregon license plate CU 21010.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

- A. Any documentation relating to AAA Financial, SAMUEL GOODWIN, CHRISTOPHER PAUL MURPHY, Kingman Arizona, Nationwide Biweekly Administration, or other documentation indicative of business ownership or incorporation.
- B. Any evidence of communication with individuals regarding the creation, distribution, receipt, transference, or solicitation of software.
- C. Any evidence of electronic or executable programs, including, but not limited to, malware, intended for use at Nationwide Biweekly Administration or any protected computer system.
- D. Log books, records, payment receipts, notes and/or customer lists, ledgers, and other papers or electronic record relating to the transportation, ordering, purchasing, processing, and distribution of controlled substances.
- E. Papers, tickets, notices, credit card receipts, travel schedules, travel receipts, passports, and/or records, and other items relating to domestic and foreign travel to obtain and distribute narcotics and narcotics proceeds, including, but not limited to airline receipts, vehicle rental receipts, truck logs, travel agency vouchers, notes, records of long distance telephone calls, e-mail and other correspondence.
- F. Address and/or telephone books and papers reflecting names, e-mail and physical addresses and/or telephone numbers of individuals, partnership, or corporations involved in cyber crimes or improper data collection from computer systems.



- G. In addition, all books, records, receipts, credit card receipts and statements, bank statements, and other related financial records, to include: currency, bank checks, money drafts, money orders, cashier's checks, and monetary instruments, including but not limited to stocks and bonds, letters of credit, receipts, passbooks, financial statements, precious metals, coins and bullion, jewelry, vehicle receipts and documents, real estate documents, documents to off-site storage facilities, safety deposit box keys, storage facility keys, utility bill statements, records of mail and answering servicing, bulk pre-paid store merchandise cards, logs, and any other items evidencing the obtaining, secreting, transfer and/or expenditures of all monetary transactions for both business and personal purposes.
- H. Electronic equipment such as pagers, computers, electric organizers, facsimile machines, cellular telephones, caller ID, telephone answering machines, police scanners, and two-way radios.
- I. Cellular telephones and portable digital assistants along with their power cords, user manuals, and software.
- J. Cellular telephone records including contracts, invoices, and documents reflecting assigned phone numbers.
- K. Internet service records including contracts, invoices, and documents reflecting assigned internet or wireless accounts.
- L. Personal income and expenditure records including uncashed checks, money orders, wire transfer records, tuition statements, check registers, bills, receipts and invoices, balance sheets, ledgers, and notes.
- M. The opening, search, and removal, if necessary, of any safe or locked receptacle or compartment, as some or all of the property heretofore may be maintained.

- N. Cash or currency in excess of \$1,000.00.
- O. Computer-related documentation or other electronic material describing the operation of any the items listed in the SUBJECT PREMISES section above, including instructions on how to access disks, files, or other material stored within same, including but not limited to computer manuals, printouts, passwords, file name lists, "readme" and/or "help files."
- P. Indicia of occupancy, residency, and/or ownership of the premises and vehicles including but not limited to utility and telephone bills, canceled envelopes, keys, deeds, tax bills, titles, and vehicle registrations.